REMARKS

The following remarks are responsive to the Non-Final Office Action of July 21, 2009 (*Office Action*).

At the time of the *Office Action*, claims 1–23 were pending. The status of the claims is as follows:

- Claims 1–3, 7–17, and 20–23 were rejected under 35 U.S.C. §112, second paragraph as being indefinite;
- Claims 1–3, 7–17, and 20–23 were rejected under 35 U.S.C. §112, first paragraph as based on a disclosure which is not enabling; and
- Claims 1–23 were rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent Publication No. 2006/0072743 to Naslund, et al (hereinafter, *Naslund*).

Applicants have amended claims 1 and 17 herein in order to more distinctly claim the invention.

35 U.S.C. §112, SECOND PARAGRAPH, INDEFINITENESS OF CLAIMS 1–3, 7–17, AND 20–23

The Examiner rejected claims 1–3, 7–17, and 20–23 as being indefinite, asserting that "per claims 1 and 17, the preamble recites that a cryptographic value (y) will be produced by the limitations of the claim. However, since only a part of the cryptographic value is produced it's unclear how it relates to (y)" (*Office Action*, pp. 2–3). Applicants amend claims 1 and 17 herein to obviate the Examiner's rejection.

Applicants have amended claims 1 and 17 to clarify that the claimed method and device, respectively, involve the production of **at least a part of** a cryptographic value (y). The language "a cryptographic value (y)" has been modified to read "at least a part of a cryptographic value (y)". At least because the claims are not directed to the production of the cryptographic value (y) itself, but rather involve the production of at least a part of the cryptographic value (y), Applicants submit that the claims as amended are definite as the claims make clear how the at least a part of the cryptographic value (y) is produced.

Based on the amendments made to claims 1 and 17, Applicants assert that the indefiniteness issues raised by the Examiner have been fully addressed such that the scope of the invention is now definite. Applicants respectfully request that this rejection be withdrawn from the *Application*.

35 U.S.C. §112, FIRST PARAGRAPH, LACK OF ENABLEMENT OF CLAIMS 1–3, 7–17, AND 20–23

The Examiner rejected claims 1–3, 7–17, and 20–23 as based on a disclosure which is not enabling, asserting that "[t]he generation of the cryptographic value being critical or essential to the practice of the invention, but not included in the claim(s) is not enabled by the disclosure" (*Office Action*, p. 3). The Examiner further asserted that "[c]laims 1 and 17 are directed to generating a cryptographic value. However, they fall short of generating the cryptographic value." Applicants amendments to claims 1 and 17 herein obviate the Examiner's rejection.

As described above, Applicants have amended claims 1 and 17 to clarify that the claimed method and device, respectively, involve the production of **at least a part** of a cryptographic value (y). The language "a cryptographic value (y)" has been modified to read "at least a part of a cryptographic value (y)". At least because the claims are not directed to the production of the cryptographic value (y) itself, but rather involve the production of **at least a part** of the cryptographic value (y), Applicants submit that the claims as amended are enabled as the claims make clear how the at least a part of the cryptographic value (y) is produced. As the Examiner acknowledged, "[t]he product of the two factors is **part of the** cryptographic value". Furthermore, the specification of the *Application* clearly provides a disclosure enabling one of ordinary skill in the art to understand how at least a part of the cryptographic value y is produced using a multiplication between the two factors, for example at page 10 line 28 – page 11 line 12 (paragraphs [0046] and [0047] of U.S. Patent Application Pub. No. 2008/0137844). Applicants note that one can claim a part of a functioning system (e.g., a steering wheel) despite the fact that the whole system (e.g., a car) is needed to actually use the part.

Based on the amendments made to claims 1 and 17, Applicants assert that the enablement issues raised by the Examiner have been fully addressed such that the scope of

the claimed invention is now enabled by the disclosure. Applicants respectfully request that this rejection be withdrawn from the *Application*.

35 U.S.C. §102(e) ANTICIPATION OF CLAIMS 1–23 BY *NASLUND*

The Examiner rejected claims 1–23 under 35 U.S.C. §102(e) as being anticipated by *Naslund*. Applicants respectfully traverse the Examiner's rejections.

Applicants note that "[a] claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987) (MPEP 2131). Applicants also note that "[t]he identical invention must be shown in as complete detail as is contained in the ... claim." *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). Further, Applicants note that "[a]ll words in a claim must be considered in judging the patentability of that claim against the prior art." *In re Wilson*, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970) (MPEP 2143.03). Additionally, Applicants note that if an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious. *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) (MPEP 2143.03).

In rejecting claims 1 and 17 as being anticipated by *Naslund*, the Examiner asserted that *Naslund* teaches "wherein said first factor comprises a determined number of bits L in a first binary representation (0132), where said second factor comprises in a second binary representation several bits set to 1 with, between each pair of consecutive bits set to 1, a sequence of at least L-1 bits set to 0 [multiple-guard bits; 0087]" (*Office Action*, pp. 5–6). Applicants traverse the Examiner's assertions.

The Examiner relied on *Naslund*'s teaching of "α" to anticipate the first factor recited in the claims, and "β" to anticipate the second factor recited in the claims. In the passages cited by the Examiner, *Naslund* teaches "the product of two (non-zero) field elements α_i and β_i in GF(p^k)" (*Naslund*, ¶[0131]) "according to the single-guard-bit representation (i.e., where guard bits of value zero are placed in . . . every successive m-th bit position) . . . can be

computed using only three table look-ups and one modular addition" (*Naslund*, ¶[0132]). *Naslund* further teaches in a multiple-guard-bit representation, "adjacent groups of bit positions 221-r are separate by a group of two guard bit positions 213-r" (*Naslund*, ¶[0087]). However, *Nasland* fails to teach the claimed relationship between the first factor and the second factor, namely that the "**second factor comprises** in a second binary representation several bits set to 1 with, between each pair of consecutive bits set to 1, **a sequence of at least L-1 bits set to 0**" where the "**first factor comprises a determined number of bits L** in a first binary representation".

Naslund teaches operations between two finite field numbers lacking a specific relationship as is specified in Applicants' claims. In particular, Applicants' claims recite a multiplication between a first factor and a second factor where the second factor's specific binary pattern is dependent on the number of bits L in the first factor. As recited in the claims, the second factor cannot be any binary representation, but must conform to a specific binary pattern. In particular, the second factor must have a pattern in which '1' bits are separated by a sequence of at least L-1 bits set to '0', wherein L is the number of bits of the first factor. *Naslund* does not teach this restriction with respect to its second factor β. In fact, *Naslund*'s first finite field element and second finite field element must have a same number of bits in order for the mathematical operations to work out. See, for example, pattern 503 in *Nasland*'s FIG. 5. In contrast, as recited in claim 1, the feature of the claims presently discussed implies that the binary representation of the second factor f2 must have a larger number of bits than the first factor f1, since the second factor comprises, in the minimum case, at least 2 bits set to '1' separated by a sequence of L-1 bits set to '0'. Therefore, when the first factor has L bits, the second factor has at least L+1 bits.

The Examiner asserted *Naslund*'s teaching of multiple guard bits in ¶[0087] as disclosing this feature of the claims. This passage merely teaches that each coefficient of a polynomial representation of a finite field element (e.g., α) is stored in a binary representation and separated from the next coefficient by several guard bits. The passage does not teach anything about the relationship between the number of guard bits used in the second finite field element β and the number of bits of the first finite field element α. On the contrary, the example described in *Naslund*'s ¶[0087] mentions two guard bits set to '0' to separate the coefficients of α, but **does not teach** that β comprises several bits set to 1 with, between each pair of consecutive bits set to 1, a sequence of at least L-1 bits set to 0 wherein α comprises

the determined number of bits L. The two guard bits set to '0' as *Naslund* teaches is much less than the total number of bits in the corresponding representation of the element, which is 16 (see e.g., FIG. 2C, which shows 16 unshaded bit positions in eight groups and two guard bits between each of the eight groups).

Applicants assert that "[t]he identical invention must be shown in as complete detail as is contained in the ... claim." *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). At least because *Naslund* fails to do so, Applicants submit that *Naslund* does not teach "wherein said first factor comprises a determined number of bits L in a first binary representation, where said second factor comprises in a second binary representation several bits set to 1 with, between each pair of consecutive bits set to 1, a sequence of at least L-1 bits set to 0" as recited in the claims.

In rejecting claims 1 and 17 as being anticipated by *Naslund*, the Examiner further asserted that *Naslund* teaches "obtaining a plurality (n) of successive binary versions of the first factor by shifting said first factor in accordance with the positions of the bits set to 1 of the second factor (shifting done in 0089)" (*Office Action* p. 6). Applicants respectfully traverse the Examiner's assertion.

As discussed previously, *Naslund* teaches the multiplication of finite field elements. In order to perform this multiplication, *Naslund* stores a first and a second finite field element in their binary form in separate registers (e.g., 109 and 111 of *Naslund*'s FIG. 1) wherein each of the first and second registers comprise k groups of data bits. Moreover, in ¶[0090], *Naslund* teaches that guard bits are used to separate each group of data bits in the first and second registers. In the passage cited by the Examiner, *Naslund* teaches "generat[ing] third binary data by executing at least one operation on contents of the first register and contents of the second register such that the k groups of first data bits are processed in parallel and such that the k groups of second data bits are processed in parallel. For example, the operation . . . can include an addition operation, a subtraction operation, a shift operation, a logical AND operation, and a NOT operation just to name a few" (*Naslund*, ¶[0089]). *Naslund* teaches that a shift operation is just one of a number of operations that may be performed. *Naslund* further discusses multiplication in paragraphs [0131] – [0150] and in FIGs. 9, 10A, and 10B. However, *Naslund* fails to specifically teach "obtaining a plurality (n) of successive binary

versions of the first factor by shifting said first factor **in accordance with the positions of the bits set to 1 of the second factor**" as recited in the claims.

The Examiner relied on *Naslund*'s general teaching of "shifting" in ¶[0089] to assert that *Naslund* teaches "obtaining a plurality (n) of successive binary versions of the first factor by shifting said first factor in accordance with the positions of the bits set to 1 of the second factor" as claimed. However, Applicants submit that *Naslund* does not disclose the specific aspects of the claims. Applicants assert that the **identical invention** must be **shown in as complete detail** as is contained in the claim. A general teaching of shifting as an operation that may be performed between two registers to perform a multiplication between two finite field elements as *Naslund* provides does not teach the elements recited in the claims in as complete detail as contained therein. Therefore, Applicants submit that *Naslund* does not teach "obtaining a plurality (n) of successive binary versions of the first factor by shifting said first factor **in accordance with the positions of the bits set to 1 of the second factor**" as the Examiner asserts.

For at least the above reasons, Applicants assert that *Naslund* does not teach the elements of claims 1 or 17. Therefore, Applicants submit that claims 1 and 17 are novel and nonobvious over the art of record, and respectfully request that the Examiner allow claims 1 and 17.

Claims 2-16 depend from claim 1, and claims 18-23 depend from claim 17. For at least the same reasons as those provided for claims 1 and 17, dependent claims 2-16 and 18-23 are novel and nonobvious over the art of record. Applicants respectfully request that the Examiner allow claims 2-16 and 18-23.

Conclusion

The application is considered in good and proper form for allowance, and the Examiner is respectfully requested to pass this application to issue. If, in the opinion of the Examiner, a telephone conference would expedite the prosecution of the subject application, the Examiner is invited to call Applicants' undersigned representative(s).

Respectfully submitted,

/brian c. rupp/

Brian C. Rupp, Reg. No. 35,665
Brent K. Whitlock, Ph.D., Reg. No. 61,371
Mark Bergner, Reg. No. 45,877
DRINKER BIDDLE & REATH LLP
191 North Wacker Drive, Suite 3700
Chicago, Illinois 60606-1698
(312) 569-1000 (telephone)
(312) 569-3000 (facsimile)
Customer No.: 08968

Date: October 19, 2009

CH01/ 25404539.1